IN THE UNITED STATES DISTRICT COURT
FOR WESTERN DISTRICT OF VIRGINIA

IN THE MATTER OF THE SEARCH OF INFORMATION REGARDING ACCOUNTS ASSOCIATED WITH CERTAIN LOCATION AND DATE INFORMATION, MAINTAINED ON COMPUTER SERVERS CONTROLLED BY GOOGLE, INC.	**FILED UNDER SEAL** Case No. 7:20mj69

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Todd Farris, being first duly sworn, hereby depose and state as follows:

Introduction and Agent Background

1. I make this affidavit in support of an application for a search warrant for information that is maintained on computer servers controlled by Google, Inc. ("Google"), an email provider headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043. The information to be searched is described in the following paragraphs and in Section I of Attachment A to the proposed warrant, which consists of Google account data associated with a particular specified location at a particular time, as specified in Section I of Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. ' 2703(c)(1)(A) to require Google to disclose to the Government copies of the information further described in Section II of Attachment A.

2. I am a Task Force Officer with the Drug Enforcement Administration, and have been since September 2013. I am currently assigned to investigate drug trafficking organizations as a member of the DEA, Washington Field Division/Roanoke Resident Office. My duties as a Task Force Officer involve the investigation of various criminal activities of narcotics traffickers and their associates. In investigating these matters, I have acted as a case agent and a contact

agent for confidential sources. These investigations have resulted in the issuance of federal search warrants, seizure warrants, indictments, and convictions of persons for federal narcotics violations. I have received training in the investigation and detection of controlled substance traffickers. I have personally conducted or assisted in over a hundred investigations into the unlawful possession, possession with the intent to distribute, and distribution of controlled substances, and the associated conspiracies to do so, to wit, violations of Title 21, United States Code Sections 841 (a)(1), and 846. Through my training and experience I have participated in investigations involving the execution of search warrants, including search warrants for electronic devices and documents. As a result of my training and experience, I am familiar with the techniques and methods of operation used by individuals involved in criminal activity to conceal their activities from detection by law enforcement authorities. Also through my training and experience I am familiar with the utilization and management of confidential sources. I am aware that confidential sources are prone to receive threats of retaliation due to their cooperation with the government during criminal investigations.

3. Based on the facts set forth in this affidavit, there is probable cause to believe that the Google accounts identified in Section I of Attachment A, associated with particular specified locations at particular specified times, contain evidence, fruits and instrumentalities of violations of Title 18, United States Code, Section 1512 (tampering with a witness) and Title 18, United States Code, Section 1513 (retaliating against a witness) (the "Subject Offenses"). .

4. This affidavit is intended only to establish sufficient probable cause for the requested search warrant and does not set forth all of my knowledge about this matter. Therefore, I have set forth only those facts necessary to support probable cause for this application. Law enforcement officers have utilized cooperating sources of information (hereinafter referred to as a CS) during this investigation. Regardless of the gender of the CS, he will be referred to in the masculine gender. The cooperating witness in this case has made statements against their own penal interest and has provided law enforcement agents with reliable and credible information which has been corroborated.

Statement of Probable Cause

5. During the time period from March 2020 through May 2020, law enforcement developed and utilized a CS to make multiple controlled purchases of heroin and fentanyl from William Preston RAMEY-WOODARD. As a result of the investigation, a federal arrest warrant was issued for RAMEY-WOODARD in the Western District of Virginia.

6. On May 20, 2020, RAMEY-WOODARD was arrested in Roanoke, Virginia on charges of distribution of heroin, distribution of fentanyl, and possession of a firearm in furtherance of a drug trafficking crime. RAMEY-WOODARD was remanded to the custody of the United States Marshals Service and is being held at the Western Virginia Regional Jail in Salem, Virginia.

7. Beginning on May 22, 2020 for three consecutive days, multiple subjects came to the residence of the CS, located at 2206 Courtland Rd., Roanoke, Virginia 24012, which is in the Western District of Virginia. During each of those occasions, the subjects yelled the CS's first name while banging on his front door in an aggressive manner. The subjects demanded that the CS answer the door. The CS refused to answer the door during each of these occasions. The CS later identified one of the subjects as Joseph Coquia MARTIN.

8. On May 31, 2020 at between approximately 10:45 pm and 11:05 pm, MARTIN returned to the CS residence and banged on the front door. MARTIN demanded that the CS answer the door. During this occasion, the CS opened the door and MARTIN entered the residence. MARTIN engaged in conversation with the CS about RAMEY-WOODARD and instructed the CS to take down his phone number in order to place a three-way phone call with RAMEY-WOODARD. At that time, the CS went back to his bedroom to retrieve his cellular phone. The CS returned from his bedroom and was met in the hallway by MARTIN, who was pointing a pistol at the CS's head. MARTIN fired a single shot at the CS, who was not struck by the round. However, the CS fell to the ground after sustaining injuries to his neck caused by the flash and burning gunpowder produced as a result of the gunshot. The CS remained on the floor and waited as MARTIN casually exited the residence. At that time, the CS called the Police, who responded shortly after receiving the emergency call.

9. During the police investigation at the CS residence, evidence technicians recovered a .45mm ammunition shell casing from inside the residence. In addition, a bullet trajectory was observed inside the residence through a coat on the wall. The investigating police officers created a photograph lineup and presented it to the CS, who was able to positively identify Joseph Coquia MARTIN as the shooter. The CS stated that he remembered MARTIN from a previous incident several years ago and was aware that MARTIN was a close friend of RAMEY-WOODARD. Based on the information obtained during the investigation, the Roanoke Police Department obtained an arrest warrant for MARTIN, who was charged with malicious wounding.

10. On June 1, 2020, law enforcement located and arrested MARTIN in the driveway of the residence located at 1628 Carrol Ave. Roanoke, VA. MARTIN was observed as the sole occupant and driver of a red Kia Soul just prior to his arrest. During a search of the vehicle, MARTIN's LG cellular phone was located and seized by law enforcement.

JURISDICTION AND AUTHORITY TO ISSUE WARRANT

1. Pursuant to 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A), the Government may require a provider of an electronic communications service or a remote computing service, such as Google, to disclose all stored content and all non-content records or other information pertaining to a subscriber, by obtaining a warrant issued using the procedures described in the Federal Rules of Criminal Procedure.

2. A search warrant under § 2703 may be issued by "any district court of the United States (including a magistrate judge of such a court)" that "has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

3. When the Government obtains records under § 2703 pursuant to a search warrant, the Government is not required to notify the subscriber of the existence of the warrant. 18 U.S.C. § 2703(a), (b)(1)(A), (c)(2) & (3). Additionally, the Government may obtain an order precluding

Google from notifying the subscriber or any other person of the warrant, for such period as the Court deems appropriate, where there is reason to believe that such notification will seriously jeopardize an investigation. 18 U.S.C. § 2705(b).

BACKGROUND RELATING TO GOOGLE, GOOGLE LOCATION SERVICES AND RELEVANT TECHNOLOGY

4. A cellular telephone or mobile telephone is a handheld wireless device primarily used for voice, text, and data communication through radio signals. Cellular telephones send signals through networks of transmitter/receivers called "cells," enabling communication with other cellular telephones or traditional "landline" telephones. Cellular telephones rely on cellular towers, the location of which may provide information on the location of the subject telephone. Cellular telephones may also include global positioning system ("GPS") technology for determining the location of the device.

5. Google is a company which, among other things, provides electronic communication services to subscribers, including email services. Google allows subscribers to obtain email accounts at the domain name gmail.com and/or google.com. Subscribers obtain an account by registering with Google. A subscriber using Google's services can access his or her email account from any computer connected to the Internet.

6. Google maintains the following records and information with respect to every subscriber account:

a. *Email contents*. In general, any email (which can include attachments such as documents, images, and videos) sent to or from a subscriber's account, or stored in draft form in the account, is maintained on Google's servers unless and until the subscriber deletes the email. If the subscriber does not delete the email, it can remain on Google's computers indefinitely. Even

if the subscriber deletes the email, it may continue to be available on Google's servers for a certain period of time.

b. *Address book.* Google also allows subscribers to maintain the equivalent of an address book, comprising email addresses and other contact information of other email users.

c. *Subscriber and billing information.* Google collects and maintains (typically unverified) identifying information about each subscriber, including, for example, name, username, address, telephone number, and alternate email addresses. Google also maintains records concerning the date on which the account was created, the Internet protocol ("IP") address of the user at the time of account creation, the current status of the account (*e.g.*, active or closed), the length of service, and the types of services utilized by the subscriber. Additionally, for paying subscribers, Google maintains records of the subscriber's means and source of payment, including any credit card or bank account number.

d. *Transactional information.* Google also typically retains certain transactional information about the use of each account on its system. This information can include records of login (*i.e.*, session) times and durations and the methods used to connect to the account (such as logging into the account through Google's website).

e. *Customer correspondence.* Google also typically maintains records of any customer service contacts with or about the subscriber, including any inquiries or complaints concerning the subscriber's account.

f. *Preserved and backup records*. Google also maintains preserved copies of the foregoing categories of records with respect to an account, for at least 90 days, upon receiving a preservation request from the Government pursuant to 18 U.S.C. § 2703(f). Google may also

maintain backup copies of the foregoing categories of records pursuant to its own data retention policy.

g. *Cookie data*. In addition, Google tracks the activity of users of their accounts, including whether or not the user of an account accesses other accounts at Google using the same computer, or mobile device. One of the ways they do that is by using Hypertext Transfer Protocol (HTTP) cookies, a string of characters stored on the user's computer, mobile device or web browser that is recognized by Google when a computer visits its site or logs into an account. Because one of the purposes of the investigation is to determine all of the accounts and means of communication used by the subjects of the investigation, both to identify the subjects and to obtain evidence of their conduct under investigation, the order calls for Google to provide records sufficient to identify those other accounts.

7. Google has developed an operating system for mobile devices, including cellular phones, known as Android that has a proprietary operating system. Nearly every cellular phone using the Android operating system has an associated Google account, and users are prompted to add a Google account when they first turn on a new Android device.

8. Based on my training and experience, I have learned that Google collects and retains location data from Android-enabled mobile devices when a Google account user has enabled Google location services. Google can also collect location data from non-Android devices if the device is registered to a Google account and the user has location services enabled. The company uses this information for location-based advertising and location-based search results. This location information is derived from a variety of sources, including GPS data, cell site/cell tower information, and Wi-Fi access points.

9. Location data can assist investigators in understanding a fuller geographic picture

and timeline, as well as possibly inculpating or exculpating account owners. Additionally, location information digitally integrated into image, video, or other computer files sent via email can further indicate the geographic location of the accounts user at a particular time (*e.g.*, digital cameras, including on cellular telephones, frequently store GPS coordinates indicating where a photo was taken in the metadata of image file).

EVIDENCE, FRUITS AND INSTRUMENTALITIES

1. Based on the foregoing, I respectfully submit that there is probable cause to believe that information stored on Google's servers associated with the Google accounts accessed at particular specified locations at particular specified times, as specified in Section I of Attachment A of the proposed warrant, will contain evidence, fruits and instrumentalities of the Subject Offenses.

2. In particular, the geographical region centered on the latitudinal and longitudinal coordinates indicated in Section I of Attachment A to the proposed warrant reflects 2206 Courtland Rd. Roanoke, Virginia 24012 at the time specified in Attachment A

3. This Application seeks authority to collect certain non-content and limited contents information related to Google accounts that were located within the Target Area during the Target Time Period (the "Subject Account"). The information sought from Google regarding the Subject Accounts, specified in indicated Section II of Attachment A to the proposed warrant, will identify (1) which cellular device MARTIN was using (if any) when he entered the residence of 2206 Courtland Rd. Roanoke, Virginia, 24012. (2) whether other individuals associated with Martin were in the area of the offense at the time of the listed offenses (3) other individuals who were in contact with MARTIN during, and therefore may have assisted him in carrying out, or have evidence of, the criminal offenses outlined in this affidavit.

4. The requested information includes:

a. *Internal Reference Number.* Unique Google-generated identification/anonymization number relating to devices used by Subject Accounts;

b. A listing of the accounts and / or devices active within the designated area within the specified time period, and the times that they were active.

c. *Location information.* All location data, whether derived from Global Positioning System (GPS) data, cell site/cell tower triangulation/trilateration, and precision measurement information such as timing advance or per call measurement data, Wi-Fi location, connection, and usage, including the GPS coordinates, estimated radius, and the dates and times of all location recordings, within the specified Target Time Period.

REQUEST FOR NON-DISCLOSURE AND SEALING

1. Based on the forgoing, I respectfully request that the Court issue the proposed search warrant. Because the warrant will be served on Google who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

2. The scope of this ongoing criminal investigation is not publicly known. As a result, premature public disclosure of this affidavit or the requested warrant could alert potential criminal targets that they are under investigation, causing them to destroy evidence, flee from prosecution, or otherwise seriously jeopardize the investigation.

3. Accordingly, there is reason to believe that, were the Provider to notify subscribers of the Subject Accounts or others of the existence of the warrant, the investigation would be seriously jeopardized. Pursuant to 18 U.S.C. § 2705(b), I therefore respectfully request

that the Court direct the Provider not to notify any person of the existence of the warrant for a period of 180 days from issuance, subject to extension upon application to the Court, if necessary.

4. For similar reasons, I respectfully request that this affidavit and all papers submitted herewith be maintained under seal until the Court orders otherwise, except that the Government be permitted without further order of this Court to provide copies of the warrant and affidavit as need be to personnel assisting it in the investigation and prosecution of this matter, and to disclose those materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

CONCLUSION

Based on the foregoing, I respectfully request that the warrant sought herein pursuant to the applicable provisions of the Stored Communications Act, 18 U.S.C. § 2703(b)(1)(A) (for contents) and § 2703(c)(1)(A) (for records and other information), and the relevant provisions of Federal Rule of Criminal Procedure 41.

Respectfully submitted,

Todd Farris
Task Force Officer
U.S. Drug Enforcement Administration

Sworn and attested to telephonically.
Subscribed and sworn to before me
on June 8, 2020:

Robert S. Ballou

The Honorable Robert S. Ballou
UNITED STATES MAGISTRATE JUDGE